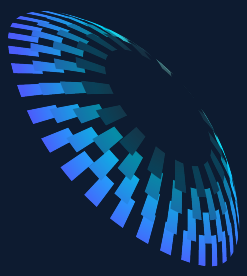

Technical Due Diligence Report

A Complete Worked Example

Distressed mid-market carve-out | Confidential | Prepared by AssetMax
Target: Meridian Packaging (Northern) Ltd | Illustrative data — fictional target

Target	Meridian Packaging (Northern) Ltd
Seller	Meridian Packaging Group PLC (manufacturing conglomerate)
Sponsor	Mid-market private equity fund (buy-side)
Enterprise value	Approx. £60m (indicative, pre-adjustment)
Report date	September 2026
Status	Confidential — for fund and adviser use only

1. Executive Summary

For fund investment committee — technology only

Headline verdict

The Target is a specialist rigid-plastics manufacturer carved out of a listed conglomerate. The business is commercially sound, but its technology estate has been run as a cost centre inside the group and is not ready for standalone operation. We assess technology risk as HIGH, driven by three ERP instances, a legacy on-premises estate, and an ageing security posture.

Three material findings

1. **ERP fragmentation**
   Three SAP instances, two unconsolidated bolt-ons, no single view of production, inventory, or finance.
2. **Legacy infrastructure**
   On-premises data centres, unsupported operating systems, no modern DR or cloud resilience.
3. **Security exposure**
   14 high-severity vulnerabilities, no enforced MFA, undocumented third-party access.

Recommendation

Proceed, subject to a £3.1m to £4.6m technology remediation provision being reflected in the purchase price, a 15-month transitional services agreement (TSA), and a dedicated carve-out IT operating plan ahead of Day 1.

2. Technology Landscape

What the company runs, and what it depends on

The Target operates six manufacturing sites across the north of England. Its application estate reflects years of group-level standardisation layered onto local improvisation. The current inventory identifies 54 business applications, of which 21 are group-shared and must be replaced or re-licensed at separation.

ERP estate

Instance	Modules	Support	Standalone readiness
SAP ECC 6.0 (primary)	Finance, production, procurement	Vendor-supported (expiring)	Ready with TSA
SAP R/3 4.7 (bolt-on A)	Partial warehouse, legacy orders	Out of support	Not standalone
SAP R/3 4.7 (bolt-on B)	Partial inventory, legacy billing	Out of support	Not standalone

Applications & data

Beyond ERP, the estate includes a custom VB6 reporting layer, two warehouse management systems, and three separate CRM instances inherited through prior acquisitions. There is no master data governance: customer, product, and vendor master data is duplicated across bolt-ons, leading to reconciliation effort at month-end and no reliable single view of margin by product line.

Infrastructure

All production workloads run on two on-premises data centres with a cold standby that has not been successfully failover-tested in over two years. Server operating systems include Windows Server 2008 R2 and 2012 (both end-of-life), and there is no public-cloud footprint. Network segmentation between OT (plant-floor) and IT is incomplete, raising the blast radius of any operational incident.

3. Architecture Assessment

Scalability, resilience, and separation readiness

The architecture is best described as a tightly-coupled, group-shaped monolith with local shadow systems. Integration runs through 86 point-to-point interfaces, many undocumented, creating a fragile dependency web that will not survive separation without explicit re-architecture.

- **Resilience**
  No active-active or automated DR; RTO for core ERP is 72+ hours against a stated target of 8. Cold standby not failover-tested in 2+ years.
- **Single points of failure**
  11 systems have a single named administrator (key-person risk); no runbook coverage for 6 of them.
- **Shared services**
  Active Directory, identity, and security tooling are group-owned and must be duplicated before Day 1.
- **Integration**
  86 point-to-point interfaces, 52 undocumented; several rely on flat-file batch transfer scheduled by hand.
- **Data architecture**
  No master data governance; duplicated masters across bolt-ons; no lineage or data-quality monitoring.
- **Scalability**
  Core ERP sized for current load with little headroom; no auto-scaling or capacity-on-demand for seasonal peaks.

Severity

Architecture risk is assessed as HIGH. The 86 interfaces and group-shared identity layer are the primary separation blockers and must be addressed inside the TSA window.

4. Technical Debt & Code Quality

Accumulated shortcuts and their remediation cost

Technical debt is material and concentrated in the two legacy bolt-on ERP instances, the custom reporting layer, and the absence of any automated testing. There is no repository-level test automation; the most complex custom code is maintained by a single contractor with no succession plan.

Debt category	Observation	Remediation
Unsupported frameworks	R/3 4.7 bolt-ons, VB6 reporting tools	£400k – £600k
Duplicated systems	Two bolt-ons duplicating core ERP function	£800k – £1.2m
Missing documentation	52 of 86 interfaces undocumented	£150k – £250k
Key-person dependency	Single contractor on core custom code	£100k – £200k
No test automation	Zero CI / unit / regression coverage	£150k – £250k

Quality signal

Code churn is concentrated in the legacy bolt-ons, which are effectively frozen in maintenance mode. New feature development has been sparse, and where it exists it is undocumented and untested. The team reports high regression risk on any change to core order-processing logic.

5. Security & Compliance

Posture, findings, and regulatory exposure

The Target's security posture is the weakest area of the review. The most recent external penetration test (2024) identified 14 high-severity, 31 medium and 48 low findings. The high-severity items remain open. Multi-factor authentication is not enforced across the estate, and at least two former group employees retain active VPN credentials.

Finding	Count	Status
High-severity vulnerabilities	14	Open (not started)
Unsupported OS (2008 R2 / 2012)	—	Live in production
MFA enforcement	—	Not deployed
Former-employee / third-party access	2+	Active VPN credentials
OT / IT segmentation	—	Incomplete

Compliance

The Target holds ISO 9001 but no current ISO 27001 or Cyber Essentials. Given the plastics supply chain, customer contracts increasingly carry security addenda; the lack of a maintained certification register is a commercial exposure that will need to be closed within the first 12 months of ownership.

Implication

Implication

The open high-severity findings are a genuine deal risk: they show the Target has had no sustained security program under group ownership, and remediation must be funded and scheduled before day one.

6. Remediation Cost Estimate

Consolidated, benchmarked, with assumptions

The table below consolidates every material finding into a quantified remediation range with a timeline. Figures are illustrative and use mid-market UK benchmarks for SAP consolidation, infrastructure rebuild, and security remediation.

Workstream	Capex	Opex	Timeline
ERP consolidation (three to one)	£1.2m – £1.8m	£200k	9 – 12 mo
Infrastructure rebuild / cloud	£600k – £900k	£150k	6 – 9 mo
Security hardening & MFA	£150k – £250k	£60k	90 days
Data migration & MDM	£300k – £450k	£40k	4 – 6 mo
Interface re-architecture	£500k – £700k	£100k	6 – 12 mo
Contingency (15%)	£410k – £645k	—	—

Scope: excludes commercial renegotiation of software licences, inflation, and any synergies from platform acquisition. Opex is annualised run-rate post-migration.

Total estimated remediation:
£3.1m – £4.6m over 12 – 18 months

7. Recommendation & TSA Handoff

Conditions to proceed and separation handoff

We recommend proceeding with the acquisition conditional on three adjustments: a price reduction reflecting the remediation provision, a 15-month TSA covering group-shared services, and a funded carve-out IT operating plan with named accountability for every separation workstream.

TSA scope (proposed)

Service	Provider	Duration	Exit trigger
ERP / core systems hosting	Seller (group IT)	15 months	ERP consolidation complete
Network & security operations	Seller (group IT)	12 months	Standalone SOC live
Active Directory / identity	Seller (group IT)	12 months	Target AD migrated
Data centre colocation	Seller (group IT)	15 months	Cloud migration done
Licence pass-through	Seller (group IT)	15 months	Direct agreements signed

Post-close priorities

- **Day 1 (0 – 90)**
  Stabilise security: close high-severity findings, enforce MFA, revoke stale access.
- **Month 3 – 6**
  Stand up standalone AD, identity, and SOC; begin data migration from bolt-ons.
- **Month 6 – 12**
  Re-architect interfaces; consolidate to a single ERP instance.
- **Month 12 – 18**
  Complete cloud re-platform and exit remaining TSA services.

Appendix: Methodology & Severity Legend

How this assessment was produced

This report follows a three-phase diligence approach. Documents were reviewed from the seller's virtual data room, supplemented by a CIO / CTO Q&A session and targeted interviews with two site IT leads. Findings were scored against a five-level severity scale and consolidated into the remediation estimate above.

Severity scale

Level	Meaning
Critical	Immediate deal or Day-1 blocking issue
High	Material cost or separation risk; must resolve in TSA window
Medium	Should resolve; manageable inside integration plan
Low	Improvement opportunity; schedule post-stabilisation

Key assumptions

- **Rates**
  Mid-market UK day rates for SAP and infrastructure specialists, 2026.
- **Scope**
  Standalone operation only; platform-acquisition synergies excluded.
- **Data**
  Bolt-on data quality assumed recoverable; no clean-room rebuild assumed.
- **Contingency**
  A flat 15% across workstreams to cover discovery during cutover.

How AssetMax Produces This Report

Diligize assembles a technical due diligence report of this depth in days rather than weeks. It inventories the application landscape, maps dependencies, quantifies technical debt against real benchmarks, and produces a remediation cost estimate specific enough to underwrite. The result is a report a deal team can act on, not a template it has to adapt.